IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS
AUSTIN DIVISION

CROGA INNOVATIONS LTD.,

Plaintiff,

v.

AMAZON WEB SERVICES, INC.,

Defendant.

Civil Action No. 1:24-CV-00398-DII

JURY TRIAL DEMANDED

MOTION OF DEFENDANT AMAZON WEB SERVICES, INC. TO DISMISS UNDER RULE 12(B)(6) FOR FAILURE TO ASSERT A PATENTABLE CLAIM

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

CASES

TABLE OF AUTHORITIES
(CONTINUED)

Page(s)

STATUTES

RULES

I. INTRODUCTION

Plaintiff Croga Innovations Limited ("Croga") alleges infringement of U.S. Patent No. 10,601,780 (the "'780 patent"), which generally relates to avoiding internet security threats. (Dkt. 1.) But the asserted '780 patent claims ineligible subject matter on its face. It purports to address the problem of internet security by limiting a host computer's access to harmful information on the internet. But the claims recite no specific, let alone new, technological solution for doing so. They instead recite a combination of functional limitations and admittedly well-understood, routine, and conventional computing components and processes, including existing firewalls and virtual computers.

Patents like Croga's—which do not provide a specific technological solution for the problem they purport to solve—are ineligible and invalid under 35 U.S.C. § 101 and a long line of Federal Circuit cases applying it. *See Affinity Labs of Tex., LLC v. Amazon.com, Inc.*, 838 F.3d 1266, 1269 (Fed. Cir. 2016); *Elec. Power Grp., LLC v. Alstom S.A.*, 830 F.3d 1350, 1356 (Fed. Cir. 2016). The Court should therefore hold the '780 patent invalid under § 101 and dismiss Croga's claims with prejudice for failure to assert a patentable claim.

II. FACTUAL BACKGROUND

Croga filed its complaint on April 16, 2024. (Dkt. 1 ("Compl.").) Croga alleges that AWS infringes "one or more claims of the '780 patent," but maps just a single claim—"exemplary independent claim 11"—against the accused AWS technology. (*Id.* ¶¶ 9-10.)

The '780 patent is titled "Internet Isolation For Avoiding Internet Security and Threats," and claims priority to an application dated January 27, 2012. ('780 patent at Cover.) As the name suggests, the patent purports to address "the protection of computer systems" and/or "local Internet networks (LANs)" "from injurious software that can be encountered while browsing or accessing the internet." (*Id.* at 1:16-20; *see also id.* at 3:6-8; 3:9-13; 12:4-6.) The specific threat the patent

describes is "harmful data"—*i.e.*, malware—that can be inadvertently "retrieved by a computer attached to and communicating over the Internet." (*Id.* at 1:25-28, 2:51-58; *see also id.* at 2:11-56 (describing malware as "toolsets" downloaded onto a host computer that allow a "remote entity" to access sensitive information on or control the host computer).) A "host computer" may become infected by either accessing a hacked website or by downloading "hidden stub code" (*e.g.*, through an email attachment). (*Id.* at 1:42-58, 1:59-2:9).

The problem of protecting computers from malware over the internet has existed since the earliest days of the internet, and, as the patent admits, many solutions to the problem already existed as of the date of the patent. (*Id.* at 2:59-60 (referencing prior art "[s]ecurity systems of various designs . . . developed to try to address the problem" of malware on the internet).) The patent describes several of these prior art systems and methods, implemented in both hardware and software. For example, a user could implement a system comprising two computers, one for accessing the internet and another, completely isolated from the internet, that only accesses a local area network. (*Id.* at 2:60-63.) According to the patent, this solution resulted "in a double cost of equipment," and created a possible "problem transferring legitimate data between the [two] machines when necessary." (*Id.* at 2:63-66.) The patent references other well-known "software-intensive methods of restricting" access to a host computer. (*Id.* at 2:66-67.) According to the patent, these existing software solutions did "not provide airtight protection" against malware, and required too much bandwidth. (*Id.* at 2:66-3:2.)

The '780 patent seeks to address these supposed shortcomings by isolating a host computer and limiting its access to the internet, using a combination of existing firewalls and a "virtual" computer. While the patent includes 20 claims, only two—claims 1 and 11—are independent. ('780 patent at 12:63-14:64.) Claim 1 recites a "networked computer system" while claim 11

recites a corresponding method. (*Id.* at 12:63-13:13; 13:65-14:16.) Claim 11, which Croga identifies as "exemplary" (Compl. ¶ 10), is reproduced below, and provides as follows:

> A method of network isolation in a networked computer system, the method comprising:
>
> *providing a network* and at least one computer system that is *configured to connect* to the network, the computer system comprising a host system and a virtual system, wherein the virtual system is a separate operating system or a software module operating on the computer system;
>
> *separating* the host system from the virtual system *using an internal firewall executed* on the computer system;
>
> *implementing network isolation* between the computer system and the network *using a host-based firewall executed* on the computer system;
>
> *providing* at least one device *configured to implement* a network firewall or a web proxy; and
>
> *implementing network isolation*, between one or more untrusted network destinations and the networked computer system, *via the at least one device*.

('780 patent, cl. 11 (emphases added).)

The claim requires: (1) a computer system connected to a network, the system consisting of both a "host system" and a "virtual system" (*i.e.*, a virtual computer); (2) limiting access between the host system and the virtual system using an "internal firewall"; (3) preventing or limiting access between the host system and the internet using another "firewall"; (4) providing a standard device configured to implement a "network firewall"; and (5) limiting access between the virtual system and the internet using the configured device.

But the claim discloses no new or specific technology for any of these elements. In fact, the patent boasts that the claimed invention can be implemented using "commercial-off-the-shelf (COTS) hardware, all of which is readily available," "standard[,] well known," and "in common use." (*Id.* at 4:50-63; *see also id.* at 7:7-10; 7:25-28; 7:45-48; 7;64-8:2; 8:6-10; 8:13-20; 9:16-19; 9:48-53; 12:53-56).) For example, the claimed "host system" can be *any* personal computer—*e.g.*,

"a PC sold by Dell," with stored "data providing an operating system that allows the host system 9 to function, e.g., a Windows or Linux operating system as is well known in the art." (*Id.* at 7:29-34.) The claimed "virtual system" is a generic software program which "may include [existing] software packages or modules such as Med-V from Microsoft, Invincea, Microsoft-Virtual PC 2007 or Hyper-V, VMWare player or ESX, or Sun Microsystems XVM Virtual Box." (*Id*. at 8:6-10.) The software program separates itself from the host by "provid[ing] an additional internal host-supported firewall"; this firewall can be any generic software used to "separate[] and restrict[] interaction between the virtual guest system 13 and the trusted-host operating system 17." (*Id.* at 8:13-17.) The specification provides no detail about *how* to accomplish this claimed separation.

The third and fifth steps of the claim require "implementing network isolation." But the specification describes only conventional technology for achieving this result. For example, the third step requires a host-based firewall to prevent or limit access between the host system and the internet. The specification describes this host-based firewall solely by reference to its function: it "provides restrictive egress from the computer" and "blocks all communications from the computer 9 except that it permits passage through it only of communications to the IP addresses of other computers on the trusted network." (*Id.* at 7:44-45; 7:49-52.) The specification admits that the host-based firewall was well-known and "implemented using software such as, for example, that sold under the names Symantec Endpoint Protection or MacAfee Host-Based Security Systems." (*Id.* at 7:45-48.)

Similarly, the fifth step requires "implementing network isolation" using a black-box device "configured to implement a network firewall or a web proxy" provided in step four. (*Id.* at 14:12-16.) The network firewall and the web proxy are also described in the specification purely by their function: they "control the type of data permitted to pass from the Internet 5 into the local

system 1, filtering e.g., pornographic material or data not intended for the system 1, and also blocks communications from users on the LAN trying to reach disallowed sites, e.g., requests to access www.onlinecasino.com." (*Id.* at 7:12-17.) The specification admits the network firewall is "of conventional configuration that is well-known in the art." (*Id.* at 7:6-9; Fig. 1.) The specification also acknowledges the web proxy is a "standard prior art security measure[] applied where the Internet meets the LAN." (*Id.* at 10:1-2; Fig. 1.) Thus, the third and fifth steps of the claim are purely functional, and the specification admits the functions can be implemented with any existing conventional technology capable of achieving the claimed results.

Independent claim 1 requires the same results recited in claim 11, implemented using generic hardware and software *configured* in an unspecified fashion. (*See id.* at cl. 1 (requiring "at least one computer system *configured to connect* to the network," "an internal firewall is *configured to separate* the host system from the virtual system," "host-based firewall . . . is *configured to implement network isolation*," "at least one device *configured to implement* at least one of a network firewall or a web proxy," and "a processor and a memory *configured to implement network isolation*") (emphases added).) In other words, the claim requires a skilled artisan to "configure" generic hardware and software elements to achieve the claimed result, and provides no actual technological solution for doing so.

The dependent claims of the '780 patent add nothing of substance to the independent claims. Several recite similar aspirational results with no description of how to achieve them. For example, dependent claims 7 and 17 require that the claimed "device" "prevent[s] unauthorized communication" "between the computer system and the one or more untrusted network destinations." (*Id.* at cls. 7, 17.) Dependent claims 4 and 14 require "wherein malware introduced to the computer system is prevented from moving to another computer system of the networked

computer system." (*Id.* at cls. 4, 14.) The claims provide no solution for either of these results.

III. ARGUMENT

The Supreme Court's opinion in *Alice* directs courts to take a two-step approach in assessing patent eligibility under § 101. *Alice Corp. Pty. Ltd. v. CLS Bank Int'l*, 573 U.S. 208, 217-18 (2014). At step one, a court must ask whether the claims are directed to a patent-ineligible abstract idea. *Id.* If they are, the court must then decide at step two whether the claims add an "inventive concept"—"an element or combination of elements that is 'sufficient to ensure that the patent in practice amounts to significantly more than a patent upon the [abstract idea] itself.'" *Id.* at 217-18 (quoting *Mayo Collaborative Servs. v. Prometheus Labs.*, 566 U.S. 66, 72-73 (2012). Unless these additional elements add something significant to the abstract idea, the claims are ineligible and invalid. *Id.* In applying the *Alice* test, the Court need not separately analyze each claim, and can instead look to representative claims. *Elec. Power Grp.*, 830 F.3d at 1351-52 & n.1.[1] The Federal Circuit has "repeatedly recognized that in many cases it is possible and proper to determine patent eligibility under 35 U.S.C. § 101 on a Rule 12(b)(6) motion."[2] *Genetic Techs. Ltd. v. Merial LLC*, 818 F.3d 1369, 1373 (Fed. Cir. 2016).

A. The claims of the '780 patent are drawn to the abstract idea of limiting access to harmful information.

In assessing whether patent claims are directed to an abstract idea at *Alice* step one, the Court examines the "focus of the claim[s]" or their "character as a whole." *Affinity Labs of Tex.,*

[1] For example, in *Content Extraction*, the district court held 242 claims from four patents invalid under § 101 based on an analysis of two representative claims, even where the parties had not agreed beforehand on the set of representative claims. *Content Extraction & Transmission LLC v. Wells Fargo Bank, N.A.*, 776 F.3d 1343, 1348 (Fed. Cir. 2014).

[2] Where, as here, "the specification admits the additional claim elements [aside from the abstract idea itself] are well-understood, routine, and conventional, it will be difficult, if not impossible, for a patentee to show a genuine dispute" of fact precluding resolution of patent eligibility on the pleadings. *Berkheimer v. HP Inc.*, 890 F.3d 1369, 1371 (Fed. Cir. 2018).

LLC v. DIRECTV, LLC, 838 F.3d 1253, 1257 (Fed. Cir. 2016); *see also BSG Tech LLC v. BuySeasons, Inc.*, 899 F.3d 1281, 1286 (Fed. Cir. 2018). In doing so, the Court must determine whether the claims recite a specific technological solution for the problem they purport to solve. *Synopsys, Inc. v. Mentor Graphics Corp.*, 839 F.3d 1138, 1151 (Fed. Cir. 2016). To be non-abstract, computer-implemented claims must be "directed to a specific improvement to computer functionality" and not merely recite "the use of conventional or generic technology in a nascent but well-known environment." *In re TLI Commc'ns LLC Pat. Litig.*, 823 F.3d 607, 612 (Fed. Cir. 2016); *see also Elec. Power Grp.*, 830 F.3d at 1356 ("[R]esult-focused, functional character of claim language has been a frequent feature of claims held ineligible under § 101, especially in the area of using generic computer and network technology to carry out economic transactions."); *Enfish, LLC v. Microsoft Corp.*, 822 F.3d 1327, 1335-36 (Fed. Cir. 2016) ("[T]he first step in the *Alice* inquiry in this case asks whether the focus of the claims is on the specific asserted improvement in computer capabilities . . . or, instead, on a process that qualifies as an 'abstract idea' for which computers are invoked merely as a tool.").

Here, the claims of the '780 patent are directed to the abstract idea of limiting access to harmful information. For example, independent claims 1 and 11 require a network-connected computer system, comprising a "host system," a "virtual system," and a series of "firewalls" that limit access between the host and virtual systems and the internet in order to protect the host system from harmful information. Access between the host system and virtual system is limited by an "internal firewall," access between the host system and the internet is limited by a "host-based firewall," and access between the virtual system and the internet is limited by a "network firewall." But the claims provide no detail about the claimed "firewalls" or their operation, and they do not describe any technological improvement to existing firewalls. Nor do they not provide any detail

about the claimed "device," or explain how to "configure" it to implement a network firewall. And the claims provide no detail about how these firewalls are used to "implement[] network isolation" between the computer system and an "untrusted network destination." They claim only the result of "network isolation" and the corresponding security benefits, while providing no specific technological solution for achieving either the results or the benefits. The dependent claims of the '780 patent recite similar aspirational results without any description of how to achieve them.[3] Such claims are abstract and ineligible as a matter of law. *Am. Axle & Mfg., Inc. v. Neapco Holdings LLC*, 967 F.3d 1285, 1302 (Fed. Cir. 2020) ("The first such requirement, that of eligibility, is that the claim itself . . . must go beyond stating a functional result; it must identify 'how' that functional result is achieved by limiting the claim scope to structures specified at some level of concreteness."); *Universal Secure Registry LLC v. Apple Inc.*, 10 F.4th 1342, 1349 (Fed. Cir. 2021) ("claims are directed to an abstract idea under *Alice* step one" when they "simply recite conventional actions in a generic way.") (internal quotation omitted); *Internet Pats. Corp. v. Active Network, Inc.*, 790 F.3d 1343, 1348 (Fed. Cir. 2015) (invalidating claims directed to a result with

[3] *See* '780 patent, cl. 2 ("internal firewall is configured to prevent data from being communicated between the virtual system and the host system without an explicit user input"), cl. 3 ("host system is configured to store data in a host memory space and the virtual system is configured to store data in a virtual memory space that is segregated from the host memory space"), cl. 4 ("malware introduced to the computer system is prevented from moving to another computer system"), cl. 5 ("computer system is configured to . . . communicate with" both "trusted" and "untrusted network destinations" using separate connections), cl. 6 ("host-based firewall is configured to prevent lateral communication and movement of malware" between devices in a computer system), cl. 7 ("device is configured to prevent unauthorized communication between the computer system and the one or more untrusted network destinations"), cl. 8 ("host-based firewall is configured to implement" a first and second "policy" permitting some communications between the host system, other computer systems on the network, and the virtual system), cl. 9 ("one or more applications or processes are configured to run in the virtual system" and "communicate with the one or more untrusted network destinations"), cl. 10 ("applications or processes are configured to run in the host system" and "communicate with one or more devices on the network"); *see also id.*, cls. 12-20 (adding nearly identical limitations to method claim 11).

"no restriction on how the result is accomplished.").

The Federal Circuit's opinion in *Dropbox, Inc. v. Synchronoss Techs., Inc.* is instructive. 815 F. App'x 529, 534 (Fed. Cir. 2020). There, the Federal Circuit held claims related to "data security" invalid under § 101. The claims recited an apparatus comprising "access control information" and an "access checker" that provided access to resources only upon meeting certain encryption and sensitivity thresholds. *Id.* at 532. The court concluded that the challenged claims were drawn to an abstract idea, noting that the claimed advance—the "access checker"—"offer[ed] nothing but a functional abstraction," and the specification described the corresponding "access filter" as simply a black box defined by its function. *Id.* at 533. While certain limitations "redirect[ed] the focus of the claims towards a technological problem [data security] . . . the claims still recite[d] no technological solution" or "specific technique" for improving a computer. *Id.* The court noted that, to claim eligible subject matter "[t]he patent has to describe *how* to solve the problem in a manner that encompasses something more than the 'principle in the abstract,'" and that "solution has to be evident from the claims." *Id*. (citation omitted). The claims of the '780 patent are no less abstract than the data security claims invalidated in *Dropbox*. Though they purport to solve the technological problem of protecting against security threats on the internet, they do not provide any specific solution for achieving this result. Like the claims held invalid in *Dropbox*, the '780 patent claims simply "recite the application of an abstract idea using conventional and well-understood techniques specified in broad, functional language." *See id.* at 534; *see also Prism Techs. LLC v. T-Mobile USA, Inc.*, 696 F. App'x 1014, 1017 (Fed. Cir. 2017) (invalidating claims directed to "providing restricted access to resources").

Because the '780 patent claims are directed to the result of limiting access to harmful information, but provide no specific solution for achieving that result, they are abstract at *Alice*

step one. *Elec. Power Grp.*, 830 F.3d at 1356.

B. The claims of the '780 patent add no inventive concept.

At *Alice* step two, the Court considers "the elements of each claim both individually and 'as an ordered combination'" to determine whether they contain an "'inventive concept' sufficient to 'transform' the claimed abstract idea into a patent-eligible application." *Alice*, 573 U.S. at 217-18, 221 (citation omitted). Neither generic computer technology, nor "well-understood, routine, conventional" components and activities, nor "purely functional" elements can supply the required inventive concept. *Id.* at 221-26 (citation omitted). To provide an inventive concept the claims of the asserted patent must claim a "technology-based solution (not an abstract-idea-based solution implemented with generic technical components in a conventional way.)" *Bascom Glob. Internet Servs., Inc. v. AT&T Mobility LLC*, 827 F.3d 1341, 1351 (Fed. Cir. 2016).

Here, the '780 patent claims merely recite the abstract idea of limiting access to harmful information, and propose to achieve this result in an unspecified manner using admittedly functional and admittedly existing, routine, and conventional computing and networking components. They add no inventive concept at *Alice* step two.

For example, independent claims 1 and 11 of the '780 patent require a "computer system" comprised of "a host system and a virtual system" connected to a "network," where the "virtual system" is an "operating system" or a "software module" separated from the "host system" "using an internal firewall," the computer system and network are isolated "using a host-based firewall" and a "device" is used to isolate "the networked computer system" from "network destinations." ('780 patent, cl. 11.) None of these limitations is inventive. The specification admits that the claimed invention can, and indeed "preferably" *should*, be "implemented by commercial-off-the shelf (COTS) hardware, all of which is readily available." (*Id.* at 4:50-52.) The patent states that "[t]he computers described herein and the networks . . . rely on the standard well known network

hardware now in common use," and "[t]he firewalls and other communication restrictions" can be implemented using existing, commercially available software. (*Id.* at 4:52-55; 4:57-59; 7:45-48.) The black box "device" required by the claims is described only as a "firewall" "of conventional configuration that is well-known in the art." (*Id.* at 7:7-10.) Such admittedly generic, conventional technology cannot provide an inventive concept as a matter of law. *Elec. Power Grp.*, 830 F.3d at 1355 ("invocation of computers, networks, and displays does not transform the claimed subject matter into patent-eligible applications"); *Apple, Inc. v. Ameranth, Inc.*, 842 F.3d 1229, 1242-42 (Fed. Cir. 2016) (finding components to be conventional where the specification "describe[d] the hardware elements of the invention as 'typical' and the software programming needed as 'commonly known.'"); *Customedia Techs., LLC v. Dish Network Corp.*, 951 F. 3d 1359, 1366 (Fed. Cir. 2020) (quoting *SAP Am. Inc. v. InvestPic, LLC*, 898 F.3d 1161, 1170 (Fed. Cir. 2018)) ("[T]he invocation of 'already-available computers that are not themselves plausibly asserted to be an advance,'" cannot save patent claims from ineligibility as this mere "'recitation of what is well-understood, routine, and conventional'" "is insufficient to supply the required inventive concept.").

The functions recited by the claim—*e.g.*, "separating the host system from the virtual system" and "implementing network isolation"—cannot provide an inventive concept because the claims provide no technical detail for implementing them. *See DIRECTV, LLC*, 838 F.3d at 1260 (lack of implementation detail for claimed inventive concept renders claim ineligible). The only descriptions of these functions in the specification refer to existing hardware and software that long predated the patent. ('780 patent at 3:25-28; 4:50-59; 7:7-10; 7:25-29; 7:45-48; 7:64-8:10; 9:16-19; 9:48-51; 11:33-36; 12:53-56.)

The dependent claims fare no better. They merely repeat functional, results-oriented steps

already recited in the independent claims. (*See supra*, note 3.) ('780 patent at 12:63-14:64.) *See DIRECTV, LLC*, 838 F.3d at 1264 ("[T]he dependent claims . . . all recite functions that are not inventive but simply constitute particular choices from within the range of existing content or hardware . . . ."). They do not add an inventive concept either.

Nor do the claims recite an inventive ordered combination of steps of components. An ordered combination lacks an inventive concept where, as here, the "recited physical components behave exactly as expected according to their ordinary use" or are "organized in a completely conventional way." *In re TLI*, 823 F.3d at 615; *see also Two-Way Media Ltd. v. Comcast Cable Commc'ns, LLC*, 874 F.3d 1329, 1341 (Fed. Cir. 2017). The functional steps and components of the '780 patent claims appear in their logical order, one inherent to the abstract idea itself—there is nothing specific or technical about the claimed arrangement of elements. *Cf. Bascom*, 827 F.3d at 1350.[4] To protect a host system or network from malware while still allowing access to the internet, there must be a separate virtual system that can be exposed to potentially harmful data, allowing for the isolation of the host system or network. There is nothing unique or inventive about the arrangement of the generic components in the claims. *See Two-Way Media*, 874 F.3d at 1339 (invalidating a "claim [that] uses a conventional ordering of steps . . . with conventional technology to achieve its desired result."); *Content Extraction*, 776 F.3d at 1348 ("well understood, routine, and conventional activities commonly used in" the relevant field do not provide an "inventive concept"). Nor does the order of limitations bring about an "unexpected result" that

[4] In *Bascom*, the challenged patent related to filtering of content over the internet. *Bascom*, 827 F.3d at 1343-44. The claims recited a system in which the filtering occurred at a remote ISP server rather than on a user's computer. *Id.* at 1344. This specific configuration—placing the filtering system on the ISP server—took "advantage of the technical capability" of the ISP servers, which could distinguish requests from various users, thus allowing for customized filtering based on the user's profile. *Id.* Unlike the claims in *Bascom*, Croga's claims recite no unique configuration and do not make use of conventional technology in an unconventional way.

"transform[s] the abstract idea into patentable subject matter." *Universal Secure Registry*, 10 F.4th at 1353, 1357-58. Indeed, the specification admits that the claimed invention does not even require any *specific* architecture, and can be applied "to a variety of host system architectures or hardware configurations." ('780 patent at 3:25-27.) The ordered combination of limitations thus cannot supply an inventive concept. The claims of the '780 patent thus fail *Alice* step two.

C. The Court should dismiss Croga's claims with prejudice, without leave to amend.

Although *Alice* step two may implicate fact issues in some cases, *Berkheimer*, 891 F.3d at 1368, here no such fact dispute precludes resolution of patent eligibility. Croga alleges no facts in its complaint that raise a fact dispute as to whether a claim element is well-understood, routine, and conventional. Nor can "any allegation about inventiveness, wholly divorced from the claims or the specification," defeat a motion to dismiss. *Cellspin Soft, Inc. v. Fitbit, Inc.*, 927 F.3d 1306, 1317 (Fed. Cir. 2019). For the same reason, the Court should not permit Croga to amend its complaint. Because no amendment could change the abstract nature of the '780 patent claims, any amendment to the complaint would be futile. *See, e.g.*, *Voip-Pal.com, Inc. v. Apple Inc.*, 375 F. Supp. 3d 1110, 1145 (N.D. Cal. 2019), *aff'd sub nom*. *Voip-Pal.com, Inc. v. Twitter, Inc.*, 798 F. App'x 644 (Fed. Cir. 2020) ("[A]ttorney argument in the complaint cannot save the claims because the purported improvements have not been captured in the claim language.").

IV. CONCLUSION

For these reasons, the Court should hold the claims of the '780 patent invalid for failure to claim patent-eligible subject matter under § 101, and dismiss Croga's claims with prejudice for failure to state a claim under Rule 12(b)(6).

Dated: July 8, 2024

Respectfully submitted,

/s/ Ravi R. Ranganath

J. David Hadden, CSB No. 176148
(Admitted W.D. Tex.)
Email: dhadden@fenwick.com
Saina S. Shamilov, CSB No. 215636
(Admitted W.D. Tex.)
Email: sshamilov@fenwick.com
Ravi R. Ranganath, CSB 272981
(Admitted W.D. Tex.)
Email: rranganath@fenwick.com
Ruchika Verma, CSB No. 311279
(Admitted W.D. Tex.)
Email: rverma@fenwick.com
FENWICK & WEST LLP
801 California Street
Mountain View, CA 94041
Telephone: 650.988.8500
Facsimile: 650.938.5200

Counsel for Defendant
AMAZON WEB SERVICES, INC.

Of Counsel:

Deron R. Dacus (TX Bar #00790553)
ddacus@dacusfirm.com
THE DACUS FIRM, P.C.
821 ESE Loop 323, Suite 430
Tyler, TX 75701
Telephone: (903) 705-1117
Facsimile: (903) 581-2543

CERTIFICATE OF SERVICE

The undersigned certifies that a true and correct copy of the above and foregoing document has been served to all counsel of record who are deemed to have consented to electronic service via the Court's CM-ECF system.

/s/ Ravi R. Ranganath
Ravi R. Ranganath